WHAT IS CLAIMED IS:

1. A security protocol structure in an application layer, comprising:

a secure session layer between a session layer and an application layer, wherein the secret session layer provides a data security function in the application layer.

2. The protocol structure of claim 1, wherein the secure session layer further comprises a secured session layer security (SSLS) protocol to provide a secret session interface to an application program.

3. The protocol structure of claim 1, further comprising a network layer, a transport layer, a security layer, and a transaction layer.

4. The protocol structure of claim 3, wherein the transport layer comprises a wireless datagram protocol, the security layer comprises a wireless transport layer security, the transaction layer comprises a wireless transaction protocol, the session layer comprises a wireless session protocol, and the application layer comprises a wireless application environment.

5. The protocol structure of claim 1, wherein a shared secret value is stored by a client and a server, and wherein the shared secret value is a pre-master secret.

6. A method of establishing a security protocol structure in an application layer, comprising:

receiving a first message containing a client random value from a client;

determining whether the first message is a valid message;

extracting a pre-master secret from the first message;

generating a specific server random value;

generating and transmitting a second message to the client to pass the server random value to the client;

generating a master secret in accordance with the extracted pre-master secret, client random value, and server random value;

generating a key block in accordance with the master secret, client random value, and server random value;

generating from the key block an encryption key value for encryption and decryption algorithms and Message Authentication Code (MAC) algorithms;

generating a third message indicating that encryption is activated; and

generating a fourth message to verify that the client has generated a client master secret identical to the master secret.

7. The method of claim 6, wherein the client random value is a client ID.

8. The method of claim 6, wherein the pre-master secret is a shared pre-master secret, and wherein the server manages the shared pre-master secret corresponding to the first message in a database.

9. The method of claim 8, wherein the first message is a user ID entered on a client terminal by a subscriber.

10. The method of claim 6, wherein the fourth message is a Finished message, and is transmitted from a record layer.

11. The method of claim 10, wherein the Finished message is transmitted using the encryption key and MAC key values, and indicates that encrypted communications have been established.

12. The method of claim 6, wherein the client computes values of the master secret, the key block, the encryption key, and the MAC key after receiving and processing the second message.

13. The method of claim 6, wherein the third message is a ChangeCipherSpec message.

14. The method of claim 6, wherein the encryption key is extracted from the key block in such a manner that a 16 byte client MAC key, 16 byte client encryption key, 8 byte client IV, 16 byte server MAC key, 16 byte server encryption key, and 8 byte server IV are sequentially allocated from the key block.

15. The method of claim 6, wherein the first message and the second message comprise a Handshake message.

16. The method of claim 15, wherein the Handshake message is formed by concatenating the first message and the second message.

17. The method of claim 6, wherein the second message is a ServerHello message, the third message is a ChangeCipherSpec message, and the fourth message is a Finished message, and wherein the second, third, and fourth messages are concatenated together to be transmitted to the client.

18. The method of claim 6, wherein the client verifies that encryption is activated after receiving and processing the third message.

19. The method of claim 6, wherein a security protocol comprises a Secured Session Layer Security protocol and the communications protocol comprises a Wireless Application Protocol.

20. The method of claim 7, wherein a subscriber inputs the client ID into a wireless communications device to establish secure communications with a server using a Wireless Application Protocol (WAP).